

# On additive shifts of multiplicative subgroups

Shkredov I.D.<sup>\*</sup>, Vyugin I.V.<sup>†</sup>

Annotation.

*Generalizing a result of S.V. Konyagin and D.R. Heath–Brown, we prove, in particular, that for any multiplicative subgroup  $R \subseteq \mathbb{Z}/p\mathbb{Z}$  and any nonzero elements  $\mu_1, \dots, \mu_k$  the following holds  $|R \cap (R + \mu_1) \cap \dots \cap (R + \mu_k)| \ll_k |R|^{\frac{1}{2} + \alpha_k}$ , provided by  $1 \ll_k |R| \ll_k p^{1 - \beta_k}$ , where  $\alpha_k, \beta_k$  are some sequences of positive reals and  $\alpha_k, \beta_k \rightarrow 0, k \rightarrow \infty$ . Besides we show that for an arbitrary subgroup  $R$ ,  $|R| \ll p^{1/2}$  one have  $|R \pm R| \gg |R|^{5/3} \log^{-1/2} |R|$ .*

## 1. Introduction.

Let  $p$  be a prime number,  $\mathbb{Z}_p^* = (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$  be the group of all invertible elements of the field  $\mathbb{Z}_p$ , and  $R \subseteq \mathbb{Z}_p^*$  be its multiplicative subgroup. Different properties of such subgroups have been studied by several authors, see e.g. [2]–[5], [7]–[14], [16], [18]. For example A. Garcia and J.F. Voloch [8], using deep algebraic ideas, proved that for any subgroup  $R$ ,  $|R| < (p - 1)/((p - 1)^{1/4} + 1)$  and an arbitrary nonzero  $\mu$  the following holds

$$|R \cap (R + \mu)| \leq 4|R|^{2/3}. \quad (1)$$

D.R. Heath–Brown and S.V. Konyagin generalized (1) and gave another prove of the result in [9] (see also [13]). Their approach uses a well-known method of S.A. Stepanov [15]. In the paper we extend the result of Garcia–Voloch and also similar theorems from [9], [13] for the case of several additive shifts. Let us formulate one of the main of our results.

**Theorem 1.1** *Let  $R \subseteq \mathbb{Z}_p^*$  be a multiplicative subgroup,  $k \geq 1$  be a positive integer,  $|R| > k2^{2k+4}$ . Let also  $\mu_1, \dots, \mu_k$  be different nonzero residuals, and  $Q = RQ$  be a  $R$ –invariant set,  $0 \notin Q$ ,  $|Q| < ((|R|/k)^{1/2k} - 1)^{2k+1}$ ,  $p \geq 4k|R|(|Q|^{\frac{1}{2k+1}} + 1)$ . Then*

$$\sum_{\lambda \in Q} |R \cap (R + \lambda \cdot \mu_1) \cap \dots \cap (R + \lambda \cdot \mu_k)| \leq 4(k + 1)(|Q|^{\frac{1}{2k+1}} + 1)^{k+1} |R|. \quad (2)$$

Theorem 1.1 easily implies a statement on the maximal cardinality of the intersection of  $k$  additive shifts of a subgroup.

**Corollary 1.2** *Let  $R \subseteq \mathbb{Z}_p^*$  be a multiplicative subgroup,  $k \geq 1$  be a positive integer, and  $\mu_1, \dots, \mu_k$  be different nonzero elements. Let also*

$$32k2^{20k \log(k+1)} \leq |R|, \quad p \geq 4k|R|(|R|^{\frac{1}{2k+1}} + 1).$$

<sup>\*</sup>The author is supported Pierre Deligne’s grant based on his 2004 Balzan prize, President’s of Russian Federation grant N –1959.2009.1, grant RFFI N 06-01-00383 and grant Leading Scientific Schools No. 8684.2010.1

<sup>†</sup>The author is supported by grant Leading Scientific Schools No. 8508.2010.1

Then

$$|R \cap (R + \mu_1) \cap \dots \cap (R + \mu_k)| \leq 4(k+1)(|R|^{\frac{1}{2k+1}} + 1)^{k+1}.$$

Roughly speaking, the corollary above asserts that  $|R \cap (R + \mu_1) \cap \dots \cap (R + \mu_k)| \ll_k |R|^{\frac{1}{2} + \alpha_k}$ , provided by  $1 \ll_k |R| \ll_k p^{1-\beta_k}$ , where  $\alpha_k, \beta_k$  are some sequences of positive numbers, and  $\alpha_k, \beta_k \rightarrow 0, k \rightarrow \infty$ .

Our approach develops the method from [9], [13].

Now consider another additive characteristic of multiplicative subgroups, namely, the cardinality of their sums and differences. Bound (1) implies that (see [8])

$$|R \pm R| \gg |R|^{4/3}$$

for any subgroup  $R$  with  $|R| \ll p^{3/4}$ . D.R. Heath–Brown and S.V. Konyagin in [9] (see also [13]) proved

$$|R \pm R| \gg |R|^{3/2} \tag{3}$$

for all subgroups  $R$  such that  $|R| \ll p^{2/3}$ . Using a combinatorial idea from [20] (see also papers [21]–[24], which are develop the approach), we improve inequality (3) (see Theorem 5.5 of section 5) in the following way

$$|R \pm R| \gg \frac{|R|^{5/3}}{\log^{1/2} |R|} \tag{4}$$

for subgroups  $R$  with the condition  $|R| \ll p^{1/2}$ .

Let us say a few words about the structure of the paper. In auxiliary section 2 we give a series of required definitions and discuss, in detail, a generalization of ordinary convolutions, which is naturally appears in the problems concerning several additive shifts. In the next section 3 we obtain preliminary results on linear dependence of some systems of polynomials in  $\mathbb{Z}_p[x]$ . Applying Stepanov’s method and using linear independence of such polynomials, we get Theorem 1.1 in the next section 4. The last section 5 contains consequences of the obtained results, and also their applications to combinatorial number theory. Here we prove, in particular, inequality (4).

We conclude with few comments regarding the notation used in this paper. Let  $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ , and  $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ . If  $A$  is a set then we write  $A(x)$  for its characteristic function. Thus  $A(x) = 1$  if  $x \in A$  and  $A(x) = 0$  otherwise. We use the symbol  $|A|$  to denote the cardinality of the set  $A$ . All logarithms  $\log$  are base 2. Signs  $\ll$  and  $\gg$  are the usual Vinogradov’s symbols. For a positive integer  $n$ , we set  $[n] = \{1, \dots, n\}$ .

The authors are grateful of S.V. Konyagin for a number of helpful advices and remarks.

## 2. Katz–Koester method and higher convolutions.

Recall the required definitions. Let  $\mathbf{G}$  be a finite Abelian group,  $N = |\mathbf{G}|$ . It is well-known [19] that the dual group  $\widehat{\mathbf{G}}$  is isomorphic to  $\mathbf{G}$ . Let  $f$  be a function from  $\mathbf{G}$  to  $\mathbb{C}$ . We denote the Fourier transform of  $f$  by  $\widehat{f}$ ,

$$\widehat{f}(\xi) = \sum_{x \in \mathbf{G}} f(x) e(-\xi \cdot x), \tag{5}$$

where  $e(x) = e^{2\pi i x}$ . Define the two convolutions of functions  $f$  and  $g$

$$(f * g)(x) := \sum_{y \in \mathbf{G}} f(y) g(x - y), \quad \text{and} \quad (f \circ g)(x) := \sum_{y \in \mathbf{G}} f(y) g(y + x).$$

Write  $E(A, B)$  for *additive energy* of two sets  $A, B \subseteq \mathbf{G}$  (see e.g. [17]), that is

$$E(A, B) = |\{a_1 + b_1 = a_2 + b_2 : a_1, a_2 \in A, b_1, b_2 \in B\}|.$$

If  $A = B$  we simply write  $E(A)$  instead of  $E(A, A)$ . Clearly,

$$E(A, B) = \sum_x (A * B)(x)^2 = \sum_x (A \circ B)(x)^2 = \sum_x (A \circ A)(x)(B \circ B)(x). \quad (6)$$

Consider a generalization of the operation  $\circ$ .

*Definition 2.1* Let  $k \geq 1$  be a positive number, and  $f_1, \dots, f_k : \mathbf{G} \rightarrow \mathbb{C}$  be functions. Denote by  $C_k(f_1, \dots, f_k)(x_1, \dots, x_{k-1})$  the function

$$C_k(f_1, \dots, f_k)(x_1, \dots, x_{k-1}) = \sum_z f_1(z) f_2(z + x_1) \dots f_k(z + x_{k-1}).$$

Thus,  $C_2(f_1, f_2)(x) = (f_1 \circ f_2)(x)$ . Put  $C_1(f) = \sum_z f(z)$ . If  $f_1 = \dots = f_k = A$ ,  $A \subseteq \mathbf{G}$  is a set then write  $C_k(A)(x_1, \dots, x_{k-1})$  for  $C_k(f_1, \dots, f_k)(x_1, \dots, x_{k-1})$ .

*Definition 2.2* Let  $A, B \subseteq \mathbf{G}$  be arbitrary sets and  $l \geq 1$  be a positive integer. Then

$$A \otimes_l B = \bigcup_{b \in B} (A - b)^l \subseteq \mathbf{G}^l. \quad (7)$$

In particular  $A \otimes_1 B = A \otimes B = A - B$ .

Clearly,

$$\text{supp } C_k(B, A, \dots, A) = \bigcup_{a \in B} (A - a)^{k-1} = A \otimes_{k-1} B \subseteq \mathbf{G}^{k-1}.$$

We have  $|A|^{k-1} \leq |A \otimes_{k-1} B| \leq |B| |A|^{k-1}$ . In particular, the set  $A \otimes_{k-1} B$  is nonempty. Let

$$E_k(f_1, \dots, f_k) = \sum_{x_1, \dots, x_{k-1}} C_k^2(f_1, \dots, f_k)(x_1, \dots, x_{k-1}).$$

Then  $E_2(A, B) = E(A, B)$ . We write  $E_k(A)$  for  $E_k(A, \dots, A)$ . There is an obvious connection between quantities  $|A \otimes_{k-1} A|$  and  $E_k(A)$ .

**Lemma 2.3** *Let  $A, B \subseteq \mathbf{G}$  be two sets, and  $k \geq 2$  be a positive integer. Then*

$$|A|^{2k-2} |B|^2 \leq E_k(A, \dots, A, B) \cdot |A \otimes_{k-1} B|.$$

**Proof.** We have  $\sum_{x_1, \dots, x_{k-1}} C_k(B, A, \dots, A)(x_1, \dots, x_{k-1}) = |A|^{k-1} |B|$ . Using Cauchy-Schwarz, we obtain the required estimate.  $\square$

Let  $B \subseteq A$  be a set, and  $(x_1, \dots, x_k) := \vec{x} \in A \otimes_{k-1} B$  be a vector. Put  $B_{\vec{x}} = B \cap (A - x_1) \cap (A - x_2) \cap \dots \cap (A - x_k)$ . Clearly,  $B_{\vec{x}}$  is nonempty. Besides  $|B_{\vec{x}}| = C_k(B, A, \dots, A)(x_1, \dots, x_{k-1})$ . We can easily describe the structure  $A \otimes_{k-1} B$  using the sets  $B_{\vec{x}}$ .

**Lemma 2.4** *Let  $B \subseteq A \subseteq \mathbf{G}$  be two sets, and  $l \geq 1$  be a positive integer. Then*

$$A \otimes_l B = \{(x_1, \dots, x_l) : A_{x_1, \dots, x_l} \bigcap B \neq \emptyset\}.$$

**Corollary 2.5** *Let  $B \subseteq A \subseteq \mathbf{G}$  be two sets, and  $l \geq 2$ ,  $m \geq 1$  be positive integers,  $m \leq l$ . Then*

$$A \otimes_l B = \bigcup_{(x_1, \dots, x_m) \in A \otimes_m B} \{(x_1, \dots, x_m)\} \times (A \otimes_{l-m} B_{x_1, \dots, x_m}). \quad (8)$$

*In particular,*

$$A \otimes_l A = \bigcup_{(x_1, \dots, x_{l-1}) \in A \otimes_{l-1} A} \{(x_1, \dots, x_{l-1})\} \times (A - A_{x_1, \dots, x_{l-1}}). \quad (9)$$

We need in upper bounds for the cardinality of  $A \otimes_{k-1} A$ . For positive integers  $l$  and  $m$ ,  $m \leq l$ , arbitrary set  $E \subseteq [l]$ ,  $E = \{j_1, \dots, j_m\}$ , and any vector  $x = (x_1, \dots, x_l)$  the symbol  $x^E$  denotes the vector  $(x_{j_1}, \dots, x_{j_m})$ . The following lemma is a consequence of the definitions.

**Lemma 2.6** *Let  $A \subseteq \mathbf{G}$  be a set, and  $l \geq 1$  be a positive integer. Let also  $S = A - A$ . Then*

$$(A \otimes_l A)(x_1, \dots, x_l) \leq \prod_{E \subseteq [l], |E|=m} (A \otimes_m A)(x^E). \quad (10)$$

*Besides*

$$(A \otimes_2 A)(x, y) \leq S(x)S(y)S(x - y), \quad (11)$$

*and*

$$(A \otimes_l A)(x_1, \dots, x_l) \leq \prod_{i,j=0, i \neq j}^k S(x_i - x_j), \quad (12)$$

*where  $x_0$  denotes 0.*

Clearly, (12) is a consequence of (10) and (11).

**Corollary 2.7** *Let  $A \subseteq \mathbf{G}$  be a set, and  $l \geq 1$  be a positive integer. Let also  $S = A - A$ . Then*

$$|A \otimes_l A| \leq \sum_{x \in S} |A - A_x|^{l-1} \leq \sum_{x \in S} (S \circ S)^{l-1}(x). \quad (13)$$

**Proof.** The first inequality in (13) is a consequence of formula (8) of Corollary 2.5, applying with  $m = 1$ . Lemma 2.6 immediately implies the bound  $|A \otimes_l A| \leq \sum_{x \in S} (S \circ S)^{l-1}(x)$ . Finally, the middle inequality is a consequence of Katz–Koester inclusion [20]

$$A_{\vec{s}} - A_{\vec{t}} \subseteq S_{\vec{u}}, \quad (14)$$

where  $\vec{s} = (s_1, \dots, s_m)$ ,  $\vec{t} = (t_1, \dots, t_n)$  are two arbitrary vectors of the lengths  $m, n$ , respectively,  $\vec{s} \in A \otimes_m A$ ,  $\vec{t} \in A \otimes_n A$ , and the vector  $\vec{u}$  has the length  $(n+1)(m+1) - 1$  and consists of all non-zero sums  $s_i + t_j$ ,  $i = 0, 1, \dots, m$ ,  $j = 0, 1, \dots, n$ .  $\square$ .

Let us generalize Lemma 3.1 from [14].

**Lemma 2.8** *Let  $A \subseteq \mathbf{G}$  be a set,  $l \geq 1$ ,  $k \geq 2$  be positive integers. Then*

$$\sum_{\vec{s}_1, \dots, \vec{s}_k} \sum_{z_1, \dots, z_{k-1}} C_k^l(A_{\vec{s}_1}, \dots, A_{\vec{s}_k})(z_1, \dots, z_{k-1}) = \sum_{x_1, \dots, x_{l-1}} C_l^{\|\vec{s}\|+k}(A)(x_1, \dots, x_{l-1}), \quad (15)$$

*where  $\|\vec{s}\| = \sum_{j=1}^k |\vec{s}_j|$ . In particular,*

$$\sum_{\vec{s}_1, \dots, \vec{s}_k} \sum_{z_1, \dots, z_{k-1}} C_k(A_{\vec{s}_1}, \dots, A_{\vec{s}_k})(z_1, \dots, z_{k-1}) = |A|^{\|\vec{s}\|+k}, \quad (16)$$

and

$$\sum_{\vec{s}_1, \dots, \vec{s}_k} \sum_{z_1, \dots, z_{k-1}} C_k^2(A_{\vec{s}_1}, \dots, A_{\vec{s}_k})(z_1, \dots, z_{k-1}) = \sum_{\vec{s}_1, \dots, \vec{s}_k} E_k(A_{\vec{s}_1}, \dots, A_{\vec{s}_k}) = E_{\|\vec{s}\|+k}(A). \quad (17)$$

**Proof.** We have (recall that  $z_0 = 0$ )

$$\begin{aligned} \sum_{\vec{s}_1, \dots, \vec{s}_k} \sum_{z_1, \dots, z_{k-1}} C_k^l(A_{\vec{s}_1}, \dots, A_{\vec{s}_k})(z_1, \dots, z_{k-1}) &= \sum_{\vec{s}_1, \dots, \vec{s}_k} \sum_{z_1, \dots, z_{k-1}} \sum_{w_1, \dots, w_l} \prod_{j=1}^l \prod_{i=1}^k A_{\vec{s}_i}(w_j + z_{i-1}) \quad (18) \\ &= \sum_{w_1, \dots, w_l} \sum_{z_1, \dots, z_{k-1}} C_k^{\|\vec{s}\|}(A)(w_2 - w_1, \dots, w_l - w_1) \prod_{j=1}^l \prod_{i=1}^k A(w_j + z_{i-1}) = \\ &= \sum_{w_1, \dots, w_l} C_k^{\|\vec{s}\|+k-1}(A)(w_2 - w_1, \dots, w_l - w_1) A(w_1) \dots A(w_l) = \sum_{x_1, \dots, x_{l-1}} C_l^{\|\vec{s}\|+k}(A)(x_1, \dots, x_{l-1}), \end{aligned}$$

because each component of any vector  $\vec{s}_i$  appears at formula (18) exactly  $l$  times. This completes the proof.  $\square$

### 3. On linear independence of a system of polynomials.

In paper [13] the following lemma was proved.

**Lemma 3.1** *Let  $\alpha_1 \in \mathbb{Z}_p^*$  be an arbitrary residual. Let also  $t, B, D$  be some positive integers,  $p$  be a prime number, and*

$$t \geq BD, \quad p \geq tB. \quad (19)$$

*Then the polynomials of the form*

$$x^{a_i} x^{tb_{0,i}} (x - \alpha_1)^{tb_{1,i}} \quad (20)$$

*where  $a_i < D$ ,  $b_{0,i}, b_{1,i} < B$  are linearly independent over  $\mathbb{Z}_p$ .*

In the section we generalize the lemma above for systems of polynomials with larger number of monomials. Our dependence between parameters worse than in Lemma 3.1.

We use the notion of formal derivative in  $\mathbb{Z}_p$ . The derivative of a polynomial is a formal derivative of the sum of its monomials, that is another polynomial

$$\left( \sum_{i=0}^n c_i x^i \right)' = \sum_{i=1}^n i c_i x^{i-1}.$$

We consider the derivatives of polynomials with the degree at most  $p-1$ . Leibniz's law holds for the formal derivative of such polynomials. Note that the derivation is well-defined for formal sums not functions.

**Proposition 3.2** *Let  $n, t, B, D$  be positive integers, and  $p$  be a prime number. Let also  $\alpha_1, \dots, \alpha_n \in \mathbb{Z}_p^*$  be different nonzero residuals, and*

$$t \geq \frac{1}{2}(n-1)B^{2n} + DB^n, \quad p \geq (2nB+2)t. \quad (21)$$

*Then the polynomials of the form*

$$x^{a_i} x^{tb_{0,i}} (x - \alpha_1)^{tb_{1,i}} \dots (x - \alpha_n)^{tb_{n,i}} \quad (22)$$

where  $a_i < D$ ,  $b_{0,i}, b_{1,i}, \dots, b_{n,i} < B$  are linearly independent over  $\mathbb{Z}_p$ .

**Proof.** Suppose that there is a nontrivial linear combination of the polynomials from (22), which equals zero identically

$$\sum_{i=1}^m C_i x^{a_i} x^{tb_{0,i}} (x - \alpha_1)^{tb_{1,i}} \dots (x - \alpha_n)^{tb_{n,i}} \equiv 0. \quad (23)$$

Divide (23) by  $(x - \alpha_n)^{ts}$ , where  $s = \min_i b_{n,i}$ . Consider the terms from (23) with minimal  $b_{n,i}$ , i.e. equal  $s$ . One can suppose that these are the first  $l_0$  terms. Then the polynomial

$$\Phi(x) = \sum_{i=1}^{l_0} C_i x^{a_i} x^{tb_{0,i}} (x - \alpha_1)^{tb_{1,i}} \dots (x - \alpha_{n-1})^{tb_{n-1,i}} \quad (24)$$

divided by  $(x - \alpha_n)^t$ . Denote the sum of polynomials from (24) with the same multiplier  $x^{tb_{0,i}} (x - \alpha_1)^{tb_{1,i}} \dots (x - \alpha_{n-1})^{tb_{n-1,i}}$  as

$$\Phi_i(x) = H_i(x) x^{tb_{0,i}} (x - \alpha_1)^{tb_{1,i}} \dots (x - \alpha_{n-1})^{tb_{n-1,i}}, \quad i = 1, \dots, l.$$

Clearly,  $\deg H_i < D$  and  $l < B^n$ . Consider Vronskian

$$W(\Phi_1, \dots, \Phi_l) = \begin{vmatrix} \Phi_1(x) & \Phi_2(x) & \dots & \Phi_l(x) \\ \Phi_1'(x) & \Phi_2'(x) & \dots & \Phi_l'(x) \\ \vdots & \vdots & \ddots & \vdots \\ \Phi_1^{(l-1)}(x) & \Phi_2^{(l)}(x) & \dots & \Phi_l^{(l-1)}(x) \end{vmatrix}. \quad (25)$$

That is a polynomial of  $x$  (let us call it  $P(x)$ ) having the degree at most

$$\deg P(x) \leq \sum_{i=1}^l \sum_{j=0}^{n-1} tb_{j,i} + l(D-1) - \frac{1}{2}l(l-1).$$

It is easy to see that  $P(x)$  divided by polynomials

$$\Psi_0(x) = x^{\sum_{i=1}^l tb_{0,i} - \frac{1}{2}l(l-1)}$$

and polynomials

$$\Psi_k(x) = (x - \alpha_k)^{(t \sum_{i=1}^l b_{k,i}) - \frac{1}{2}l(l-1)}, \quad k = 1, \dots, n-1,$$

which are called  $\Psi_0(x), \dots, \Psi_{n-1}(x)$ . Thus  $P(x)$  divided by

$$\Psi(x) = \prod_{k=0}^{n-1} \Psi_k(x).$$

At the same time

$$\deg \Psi(x) = \sum_{i=1}^l tb_{0,i} + t \sum_{k=1}^{n-1} \sum_{i=1}^l b_{k,i} - \frac{1}{2}nl(l-1) = \deg P(x) - \frac{1}{2}(n-1)l(l-1) - l(D-1).$$

It remains to note that if  $P(x)$  is divided by  $(x - \alpha_n)^C$  then  $P(x)/\Psi(x)$  is divided by the same monomial and

$$\deg(P(x)/\Psi(x)) \leq \frac{1}{2}(n-1)l(l-1) + l(D-1).$$

Hence either  $C \leq \frac{1}{2}(n-1)l(l-1)$  or  $P(x) \equiv 0$  but in the case the polynomials  $\Phi_1(x), \dots, \Phi_l(x)$  are linearly dependent (see Lemma 3.4 below) and we reduce the original problem to the question with the smaller number of brackets.

Now return to our suggestion that the sum  $\Phi(x)$  from (24) is divided by  $(x - \alpha_n)^t$ . In the case Vronskian  $P(x) = W(\Phi_1, \dots, \Phi_l)$  is divided by  $(x - \alpha_n)^{t-(l-1)}$  because of the polynomials  $\Phi(x), \dots, \Phi^{(l-1)}(x)$  are divided by  $(x - \alpha_n)^{t-(l-1)}$ . Thus

$$t \leq (l-1) + \frac{1}{2}(n-1)l(l-1) + l(D-1) < \frac{1}{2}(n-1)l(l-1) + lD.$$

On the other hand the total number  $l$  of the polynomials  $l$  in (24) is bounded by  $l < B^n$ . Hence

$$t < \frac{1}{2}(n-1)B^{2n} + DB^n$$

with contradiction. This completes the proof.  $\square$

We give two lemmas on linear independence. Lemma 3.3 is a simple general statement and Lemma 3.4 allows us to have better dependence between parameters  $p, t, n$ , and  $B$ .

**Lemma 3.3** *Let Vronskian  $P(x) = W(\Phi_1(x), \dots, \Phi_l(x))$  of degree less than  $p$  equals zero in  $\mathbb{Z}_p[x]$ . Then there is a nontrivial linear combination of the polynomials  $\Phi_1(x), \dots, \Phi_l(x)$  with coefficients from  $\mathbb{Z}_p$  such that*

$$\mu_1\Phi_1(x) + \dots + \mu_l\Phi_l(x) \equiv 0, \quad \mu_1, \dots, \mu_l \in \mathbb{Z}_p.$$

$\square$

**Lemma 3.4** *Suppose that the notation of Proposition 3.2 holds. Let Vronskian  $P(x) = W(\Phi_1(x), \dots, \Phi_l(x))$  equals zero in  $\mathbb{Z}_p[x]$*

$$P(x) \equiv 0.$$

*Then there is a nontrivial linear combination of the polynomials  $\Phi_1(x), \dots, \Phi_l(x)$  with coefficients  $\mu_i \in \mathbb{Z}_p$ ,  $i \in [l]$  such that*

$$\mu_1\Phi_1(x) + \dots + \mu_l\Phi_l(x) \equiv 0,$$

*provided by  $p \geq (2nB + 2)t$ .*

**Proof.** Since  $P(x) \equiv 0$  it follows that there is a nontrivial zero combination of its rows, i.e.

$$\lambda_1\Phi_k(x) + \lambda_2\Phi'_k(x) + \dots + \lambda_l\Phi_k^{(l-1)}(x) \equiv 0, \quad k = 1, \dots, l, \quad (26)$$

where the coefficients  $\lambda_i = \lambda_i(x)$  depend on  $x$ , in general, and does not equal zero simultaneously. We prove that the coefficients  $\lambda_i$  can be chosen do not depend of  $x$  and does not equal zero simultaneously. Linear combination (26) can be considered as a formal linear differential equation of the order at most  $l-1$ :

$$\lambda_1 u(x) + \lambda_2 u'(x) + \dots + \lambda_l u^{(l-1)}(x) = 0. \quad (27)$$

Polynomials  $u(x)$ , satisfying the last equation form a linear space. It is easy to see that any solution of (27) having  $l - 1$  derivatives at some point  $x_0$  equal zero is equal to zero identically. Indeed, putting, say,  $x_0 = 0$  in (27), we get a linear relation between  $u^{(l-1)}(0)$  and  $u^{(l-1)}(0), \dots, u(0)$ . Taking the formal derivation of (27), we obtain similar relations for  $u^{(l)}(0)$  and so on. Thus all derivations of  $u$  are zero because they can be expressed as linear combinations of  $u^{(l-1)}(0), \dots, u(0)$ . We will prove below that the degrees of the functions  $\lambda_i(x)$  as well as linear combination (27) is less than  $p$ . Thus we can take the formal derivations of all these functions and apply the previous arguments.

Now consider a linear combination of columns of the Vronskian at the point  $x = 0$ . By assumption we have for some  $\mu_1, \dots, \mu_l$  that

$$\mu_1 \Phi_1^{(k)}(0) + \mu_2 \Phi_2^{(k)}(0) + \dots + \mu_l \Phi_l^{(k)}(0) = 0, \quad k = 0, 1, \dots, l - 1.$$

Consider the solution

$$u(x) = \mu_1 \Phi_1(x) + \mu_2 \Phi_2(x) + \dots + \mu_l \Phi_l(x)$$

of equation (27). Then  $u(0), \dots, u^{(l-1)}(0)$  equal zero. By the previous arguments  $u(x) \equiv 0$ . Thus we have found a zero linear combination of the polynomials  $\Phi_1(x), \dots, \Phi_l(x)$  with coefficients  $\mu_1, \dots, \mu_l \in \mathbb{Z}_p$  and we are done.

It is remain to show that the left hand side of equation (27) is a polynomial of degree less than  $p$ .

**Lemma 3.5** *The degree of the polynomial*

$$\lambda_1 u(x) + \lambda_2 u'(x) + \dots + \lambda_l u^{(l-1)}(x)$$

less than  $(2nB + 2)t$ .

**Proof.** The coefficients  $\lambda_1, \dots, \lambda_l$  are solutions of homogeneous system of linear equations (26). Clearly, system (26) has a nonzero solution for all  $x$ . We will use Cramer's rule. Suppose that there are  $l_1$  linear independent equations among  $l$  equations of the system. Without loss of generality one can suppose that these are the first  $l_1$  equations. Further there exist  $l_1$  columns of the matrix of system (26) such that the matrix formed by the elements of the first  $l_1$  rows and these  $l_1$  columns is non-degenerate for some  $x$ . By  $i_1, \dots, i_{l_1}$  denote the indexes of the columns and let  $j_1, \dots, j_{l-l_1}$  be the indexes of another columns. Let us solve system (26). We have

$$\lambda_{i_1} \Phi_k^{(i_1-1)}(x) + \dots + \lambda_{i_{l_1}} \Phi_k^{(i_{l_1}-1)}(x) = - \sum_{s=1}^{l-l_1} \lambda_{j_s} \Phi_k^{(j_s-1)}(x) = \hat{\Phi}_k(x), \quad k = 1, \dots, l_1,$$

where

$$\hat{\Phi}_k(x) = - \sum_{s=1}^{l-l_1} \lambda_{j_s} \Phi_k^{(j_s-1)}(x), \quad k = 1, \dots, l_1.$$

The solutions of the system form a linear space of the dimension  $l - l_1$ . Put  $\lambda_{j_1}, \dots, \lambda_{j_{l-l_1}}$  equal

$$\lambda_{j_s} = \frac{x^{D+tB} \prod_{j=1}^{n-1} (x - \alpha_j)^{tB}}{\hat{\Psi}(x)} \begin{vmatrix} \Phi_1^{(i_1-1)}(x) & \dots & \Phi_{l_1}^{(i_1-1)}(x) \\ \dots & \dots & \dots \\ \Phi_1^{(i_{l_1}-1)}(x) & \dots & \Phi_{l_1}^{(i_{l_1}-1)}(x) \end{vmatrix}, \quad s = 1, \dots, l - l_1,$$



where

$$\hat{\Psi}(x) = x^{\sum_{q=1}^{l_1} (c_q + tb_{0,q}) - \sum_{q=1}^{l_1} (i_{l_1} - i_q)} \prod_{j=1}^{n-1} (x - \alpha_j)^{(t \sum_{q=1}^{l_1} b_{j,q}) - \sum_{q=1}^{l_1} (i_{l_1} - i_q)},$$

where  $c_q = \deg H_q < D$ . Then by Cramer's rule for  $i = 1, \dots, l-1$ , we obtain

$$\lambda_{i_s} = \frac{x^{D+tB} \prod_{j=1}^{n-1} (x - \alpha_j)^{tB}}{\Psi(x)} \begin{vmatrix} \Phi_1^{(i_1-1)}(x) & \dots & \Phi_{l_1}^{(i_1-1)}(x) \\ \dots & \dots & \dots \\ \Phi_1^{(i_{s-1}-1)}(x) & \dots & \Phi_{l_1}^{(i_{s-1}-1)}(x) \\ \hat{\Phi}_1^*(x) & \dots & \hat{\Phi}_{l_1}^*(x) \\ \Phi_1^{(i_{s+1}-1)}(x) & \dots & \Phi_{l_1}^{(i_{s+1}-1)}(x) \\ \dots & \dots & \dots \\ \Phi_1^{(i_{l_1}-1)}(x) & \dots & \Phi_{l_1}^{(i_{l_1}-1)}(x) \end{vmatrix}, \quad s = 1, \dots, l_1,$$

where

$$\hat{\Phi}_k^*(x) = - \sum_{s=1}^{l-l_1} \Phi_k^{(j_s-1)}(x), \quad k = 1, \dots, l_1.$$

It is easy to see that all  $\lambda_1, \dots, \lambda_l$  are polynomials. Let us find an upper bound for the degrees of such polynomials

$$\deg \lambda_i(x) \leq \frac{1}{2} l(l-1)(n-1) + (l+1)D + nBt < (nB+1)t, \quad i = 1, \dots, l;$$

The degree of each  $\Phi_k(x)$  does not exceed

$$\deg \Phi_k(x) < nBt + D,$$

hence

$$\deg(\lambda_1 \Phi_k(x) + \lambda_2 \Phi_k'(x) + \dots + \lambda_l \Phi_k^{(l-1)}(x)) < 2ntB + t + D - 1 < (2nB+2)t,$$

as required.  $\square$

*Note 3.6* Proposition 3.2 can be proven using Fuchs equation for Levelt's basis (see the formulation in [1]). Nevertheless, we prefer to use a more simple approach calculating the degree of Vronskian of the system of the polynomials from (22).

Similarly, we obtain the following proposition.

**Proposition 3.7** *Let  $n, t, B, D, D < t$  be positive integers, and  $p$  be a prime number. Let also  $T$  be a set,  $T \subseteq \mathbb{Z}_p^*$ ,  $T > n-1$ . Finally, suppose that*

$$t \geq DB^n + \frac{\frac{n}{2} D^2 B^{2n}}{|T| - n + 1}, \quad p \geq \min\{tnDB^{n+1}, B^2 t^2 n^2\}. \quad (28)$$

*Then there is a tuple  $\alpha_1, \dots, \alpha_n \in T$  such that the polynomials of the form*

$$x^{a_i} x^{tb_{0,i}} (x - \alpha_1)^{tb_{1,i}} \dots (x - \alpha_n)^{tb_{n,i}} \quad (29)$$

*where  $a_i < D$ ,  $b_{0,i}, b_{1,i}, \dots, b_{n,i} < B$  are linearly independent over  $\mathbb{Z}_p$ .*

**Proof.** One can suppose that for some  $\alpha_1, \dots, \alpha_{n-1} \in T$  the correspondent polynomials from (29) are linearly independent over  $\mathbb{Z}_p$ , otherwise we have a problem with smaller number of

brackets. Thus, fix  $\alpha_1, \dots, \alpha_{n-1} \in T$  and let  $\alpha_n$  belongs to the nonempty set  $T \setminus \{\alpha_1, \dots, \alpha_{n-1}\}$ . After that apply the arguments as in Proposition 3.2. Suppose that there is a nontrivial linear combination of the polynomials from (29) which equals zero identically

$$\sum_{i=1}^m C_i x^{a_i} x^{tb_{0,i}} (x - \alpha_1)^{tb_{1,i}} \dots (x - \alpha_n)^{tb_{n,i}} \equiv 0. \quad (30)$$

Divide (30) by  $(x - \alpha_n)^{ts}$ , where  $s = \min_i b_{n,i}$ . Consider the terms from (30) with minimal  $b_{n,i}$ , i.e. equal  $s$ . One can suppose that these are the first  $l$  terms. Then the polynomial

$$\Phi(x) = \sum_{i=1}^l C_i x^{a_i} x^{tb_{0,i}} (x - \alpha_1)^{tb_{1,i}} \dots (x - \alpha_{n-1})^{tb_{n-1,i}} \quad (31)$$

divided by  $(x - \alpha_n)^t$ . Denote the sum of polynomials from (31) by

$$\Phi_i(x) = x^{a_i} x^{tb_{0,i}} (x - \alpha_1)^{tb_{1,i}} \dots (x - \alpha_{n-1})^{tb_{n-1,i}}, \quad i = 1, \dots, l.$$

Consider Wronskian

$$W(\Phi_1, \dots, \Phi_l) = \begin{vmatrix} \Phi_1(x) & \Phi_2(x) & \dots & \Phi_l(x) \\ \Phi_1'(x) & \Phi_2'(x) & \dots & \Phi_l'(x) \\ \vdots & \vdots & \ddots & \vdots \\ \Phi_1^{(l-1)}(x) & \Phi_2^{(l)}(x) & \dots & \Phi_l^{(l-1)}(x) \end{vmatrix}. \quad (32)$$

That is a polynomial of  $x$  (let us call it  $P(x)$ ) having the degree at most

$$\deg P(x) \leq \sum_{i=1}^l \left( a_i + t \sum_{j=0}^{n-1} b_{j,i} \right) - \frac{1}{2} l(l-1).$$

It is easy to see that  $P(x)$  divided by polynomials

$$\Psi_0(x) = x^{\sum_{i=1}^l (a_i + tb_{0,i}) - \frac{1}{2} l(l-1)}$$

and polynomials

$$\Psi_k(x) = (x - \alpha_k)^{(t \sum_{i=1}^l b_{k,i}) - \frac{1}{2} l(l-1)}, \quad k = 1, \dots, n-1,$$

which are called  $\Psi_0(x), \dots, \Psi_{n-1}(x)$ . Thus  $P(x)$  divided by

$$\Psi(x) = \prod_{k=0}^{n-1} \Psi_k(x).$$

At the same time

$$\deg \Psi(x) = \sum_{i=1}^l (a_i + tb_{0,i}) + t \sum_{k=1}^{n-1} \sum_{i=1}^l b_{k,i} - \frac{1}{2} nl(l-1) = \deg P(x) - \frac{1}{2} (n-1)l(l-1).$$

It is remain to note that if  $P(x)$  divided by  $(x - \alpha_n)^C$  then  $P(x)/\Psi(x)$  divided by the same monomial and

$$\deg(P(x)/\Psi(x)) \leq \frac{1}{2}(n-1)l(l-1).$$

Hence  $C \leq \frac{1}{2}(n-1)l(l-1)$ . Note that the polynomial  $P(x)$  does not equal zero identically because in the case the polynomials  $\Phi_1(x), \dots, \Phi_l(x)$  are linearly dependent and we obtain a contradiction (see Lemma 3.3 or Lemma 3.4).

Now return to our suggestion that the sum  $\Phi(x)$  from (31) divided by  $(x - \alpha_n)^t$ . In the case Vronskian  $P(x) = W(\Phi_1, \dots, \Phi_l)$  divided by  $(x - \alpha_n)^{t-(l-1)}$  because of the polynomials  $\Phi(x), \dots, \Phi^{(l-1)}(x)$  divided by  $(x - \alpha_n)^{t-(l-1)}$ . Thus for every  $\alpha_n$  Vronskian  $P(x) = W(\Phi_1, \dots, \Phi_l)$  divided by  $(x - \alpha_n)^{t-(l-1)}$ . Whence

$$(|T| - n + 1)(t - (l - 1)) \leq (l - 1) + \frac{1}{2}(n - 1)l(l - 1) + l(D - 1) < \frac{1}{2}(n - 1)l(l - 1) + lD.$$

On the other hand the total number of polynomials  $l$  in (31) equals  $DB^n$ . Hence

$$t < DB^n + \frac{\frac{n}{2}D^2B^{2n}}{|T| - n + 1}$$

with contradiction.

Note also

$$\deg P(x) \leq \min\{tnDB^{n+1}, B^2t^2n^2\} < p.$$

This completes the proof.  $\square$

#### 4. The proof of the main result.

Let  $R \subseteq \mathbb{Z}_p^*$  be a multiplicative subgroup, and  $t = |R|$ . Let  $k \geq 1$  be a positive integer, and  $\mu_1, \dots, \mu_k$  be fixed different nonzero elements. Let also  $\xi_0, \xi_1, \dots, \xi_k$  be some nonzero residuals, and  $A_{\vec{\xi}, \lambda}$ ,  $\vec{\xi} = (\xi_0, \xi_1, \dots, \xi_k)$ ,  $\lambda \in \mathbb{Z}_p^*$  be arbitrary subsets of the set  $\xi_0 R \cap (\xi_1 R + \lambda \cdot \mu_1) \cap \dots \cap (\xi_k R + \lambda \cdot \mu_k)$ . Finally, suppose that we have a family of sets  $A_{\vec{\xi}_1, \lambda_1}, \dots, A_{\vec{\xi}_s, \lambda_s}$ , where the sets  $A_{\vec{\xi}_l, \lambda_l}$  can have the same  $\lambda_l$ .

Applying Stepanov's method, we prove one of the main lemmas of the section. We use arguments from [13] (see also [9]).

**Lemma 4.1** *Let  $R \subseteq \mathbb{Z}_p^*$  be a multiplicative subgroup, and  $t = |R|$ . Let  $k \geq 2$ ,  $s$ ,  $B$  be arbitrary positive integers such that*

$$kB^{2k} < t, \quad ts < B^{2k+1}, \quad (33)$$

and

$$p \geq (2kB + 2)t. \quad (34)$$

Let also  $A_{\vec{\xi}_1, \lambda_1}, \dots, A_{\vec{\xi}_s, \lambda_s}$  be some sets of the family above. Then

$$\sum_{l=1}^s |A_{\vec{\xi}_l, \lambda_l}| \leq \frac{(k+1)tB}{\lfloor t/2B^k \rfloor}. \quad (35)$$

**Proof.** Let  $D = \lfloor t/(2B^k) \rfloor$ . Since  $2B^k \leq kB^{2k} < t$  it follows that  $D \geq 1$ . Let also  $\mathcal{E}$  be the union of all sets  $A_{\vec{\xi}_l, \lambda_l}$ . One can assume that the sets  $A_{\vec{\xi}_l, \lambda_l}$  are disjoint, and  $\lambda = 1$ . We need to estimate the size of the set  $\mathcal{E}$ . Let  $\Phi(X, Y, Z_1, \dots, Z_k) \in \mathbb{Z}_p[X, Y, Z_1, \dots, Z_k]$  be an arbitrary polynomial such that

$$\deg_X \Phi < D, \quad \deg_Y \Phi < B, \quad \deg_{Z_j} \Phi < B, \quad j \in [k].$$

We have

$$\Phi(X, Y, Z_1, \dots, Z_k) = \sum_{a,b,\vec{c}} \lambda_{a,b,\vec{c}} X^a Y^b Z^{\vec{c}}, \quad (36)$$

where  $\vec{c} = (c_1, \dots, c_k) \in \mathbb{Z}_p^k$  and  $Z^{\vec{c}} = Z_1^{c_1} \dots Z_k^{c_k}$ . Besides

$$\Psi(X) = \Phi(X, X^t, (X - \mu_1)^t, \dots, (X - \mu_k)^t). \quad (37)$$

Clearly

$$\deg \Psi \leq D - 1 + (k + 1)t(B - 1).$$

If we will find the coefficients  $\lambda_{a,b,\vec{c}}$  such that, firstly, the polynomial  $\Psi$  is nonzero, and, secondly,  $\Psi$  has the root of order at least  $D$  at any point of the set  $\mathcal{E}$  then

$$|\mathcal{E}| \leq (D - 1 + (k + 1)t(B - 1))/D < \frac{(k + 1)tB}{\lfloor t/2B^k \rfloor}$$

and lemma will be proved. Thus, we should check that

$$\left( \frac{d}{dX} \right)^n \Psi(X) \Big|_{X=x} = 0, \quad \forall n < D, \quad \forall x \in \mathcal{E}.$$

For any  $x \in \mathcal{E}$ , we have  $x \neq 0$  and  $x \neq \mu_j$ ,  $j \in [k]$ . Hence the last condition is equivalent

$$[X(X - \mu_1) \dots (X - \mu_k)]^n \left( \frac{d}{dX} \right)^n \Psi(X) \Big|_{X=x} = 0, \quad \forall n < D, \quad \forall x \in \mathcal{E}. \quad (38)$$

It is easy to see that for all  $m, q$ ,  $q \geq m$ , and any  $\mu$  the following holds

$$(X - \mu)^m \left( \frac{d}{dX} \right)^m (X - \mu)^q = \frac{q!}{(q - m)!} (X - \mu)^q.$$

If  $m > q$  then the left hand side equals zero. So, there are well-defined polynomials  $P_{n,a,b,\vec{c}}(X)$  such that

$$\begin{aligned} [X(X - \mu_1) \dots (X - \mu_k)]^n \left( \frac{d}{dX} \right)^n X^a X^{tb} (X - \mu_1)^{tc_1} \dots (X - \mu_k)^{tc_k} &= \\ &= P_{n,a,b,\vec{c}}(X) X^{tb} (X - \mu_1)^{tc_1} \dots (X - \mu_k)^{tc_k}. \end{aligned}$$

Here  $a, b, c_1, \dots, c_k$  are nonnegative integers. For some  $a, b, \vec{c}$  polynomial  $P_{n,a,b,\vec{c}}$  can be identically zero. Clearly,  $\deg P_{n,a,b,\vec{c}} \leq a + n$ . By the definition of the sets  $\mathcal{E}$  and  $A_{\vec{\xi}_l, \vec{\mu}_l}$ , we have

$$\begin{aligned} [X(X - \mu_1) \dots (X - \mu_k)]^n \left( \frac{d}{dX} \right)^n X^a X^{tb} (X - \mu_1)^{tc_1} \dots (X - \mu_k)^{tc_k} \Big|_{X=x} &= \\ &= y_0^b(l) y_1^{c_1}(l) \dots y_1^{c_k}(l) P_{n,a,b,\vec{c}}(X), \quad x \in A_{\vec{\xi}_l, \vec{\mu}_l}, \end{aligned}$$

where residuals  $y_0^b(l), y_1^{c_1}(l), \dots, y_1^{c_k}(l)$  does not depend on the choice of the element  $x \in A_{\vec{\xi}_l, \vec{\mu}_l}$ . By (36), (37)

$$[X(X - \mu_1) \dots (X - \mu_k)]^n \left( \frac{d}{dX} \right)^n \Psi(X) \Big|_{X=x} =$$

$$= \sum_{a,b,\vec{c}} \lambda_{a,b,\vec{c}} \cdot y_0^b(l) y_1^{c_1}(l) \dots y_1^{c_k}(l) P_{n,a,b,\vec{c}}(x) := P_{n,l}(x), \quad x \in A_{\vec{\xi}_l, \vec{\mu}_l}.$$

Coefficients of the polynomials  $P_{n,l}(X)$  are linear forms of  $\lambda_{a,b,\vec{c}}$ . Choose  $\lambda_{a,b,\vec{c}}$  such that polynomials  $P_{n,l}(X)$  are identically zero for an arbitrary  $n < D$  and any  $l \in [s]$ . Then equality (38) holds for all  $x \in \mathcal{E}$ . We have (33). Since  $\deg P_{n,l} < 2D$  it follows that

$$2sD^2 \leq 2sDt/2B^k < DB^{k+1}, \quad (39)$$

and (39) guarantee that there is a nonzero tuple of coefficients  $\lambda_{a,b,\vec{c}}$  such that  $P_{n,l}(X) \equiv 0$ ,  $n < D$ ,  $l \in [s]$ .

We must check that the obtained polynomial  $\Psi(X)$  is nonzero. We have  $D = \lceil t/(2B^k) \rceil$ , and  $kB^{2k} < t$ . Hence  $t \geq \frac{1}{2}(k-1)B^{2k} + DB^k$ . Besides inequality (34) holds. Using Proposition 3.2 with  $n = k$ , we obtain that the polynomial  $\Psi(X)$  is nonzero identically. This concludes the proof of the lemma.  $\square$

**Proof of Theorem 1.1.** Let  $|R| = t$ ,  $s = |Q|/t$ . Let  $B$  be the least integer such that  $B^{2k+1} > ts$ . Then  $B \leq (ts)^{1/(2k+1)} + 1$ . Using bound

$$|Q| < ((t/k)^{1/2k} - 1)^{2k+1},$$

we get

$$kB^{2k} \leq k((ts)^{1/(2k+1)} + 1)^{2k} < t$$

and condition (33) of Lemma 4.1 is satisfied. Since  $t > k2^{2k+4}$  and

$$|Q| < ((t/k)^{1/2k} - 1)^{2k+1} < (t/k)^{(2k+1)/2k},$$

it follows that  $t/2B^k \geq 2$ . Finally, inequality (34) of the same Lemma is a consequence of  $p \geq 4tk(|Q|^{\frac{1}{2k+1}} + 1)$ . Applying the lemma and using the bounds  $t/2B^k \geq 2$ ,  $B \leq |Q|^{\frac{1}{2k+1}} + 1$ , we obtain

$$\sum_{\lambda \in Q} |R \cap (R + \lambda \cdot \mu_1) \cap \dots \cap (R + \lambda \cdot \mu_k)| \leq t \frac{(k+1)tB}{\lfloor t/2B^k \rfloor} \leq 4(k+1)B^{k+1}t \leq 4(k+1)(|Q|^{\frac{1}{2k+1}} + 1)^{k+1}t.$$

This completes the proof.  $\square$

**Proof of Corollary 1.2.** It is sufficiently to check that for all  $|R| \geq 32k2^{20k \log(k+1)} > k2^{2k+4}$  the following holds

$$|R| < ((|R|/k)^{1/2k} - 1)^{2k+1}.$$

It is easy to see that the assumed bounds for the cardinality of  $R$  imply the last inequality.  $\square$

Using Proposition 3.7 instead of Proposition 3.2, we obtain the following statement.

**Statement 4.2** *Let  $k \geq 2$  be a positive integer, and  $R \subseteq \mathbb{Z}_p^*$  be a multiplicative subgroup. Let also  $T \subseteq \mathbb{Z}_p^*$  be any set,  $2k \leq |T| \leq |R|k/2$ , and let  $s, B$  be arbitrary natural numbers such that*

$$2kB^{2k} \leq |R||T|, \quad 2s \left( \frac{|R||T|}{2k} \right)^{1/2} < B^{2k+1}, \quad (40)$$

and

$$p \geq (2kB + 2)t. \quad (41)$$

Then there are different elements  $\mu_j \in T$ ,  $j \in [k]$  such that for all sets  $A_{\xi_1, \lambda_1}, \dots, A_{\xi_s, \lambda_s}$  the following holds

$$\sum_{l=1}^s |A_{\xi_l, \lambda_l}| \leq \frac{(k+1)|R|B}{[(|R||T|/(2kB^{2k}))^{1/2}]}. \quad (42)$$

**Proof.** Let  $t = |R|$ , and  $D = [(t|T|/(2kB^{2k}))^{1/2}]$ . Since  $2kB^{2k} \leq t|T|$  it follows that  $D \geq 1$ . Besides  $D < t$  because of  $|T| \leq tk/2$ . Let also  $\mathcal{E}$  be the union of all sets  $A_{\xi_l, \lambda_l}$ . Using the arguments as in Lemma 4.1, we construct a polynomial  $\Psi$ , having a root of order at least  $D$  at any point of the set  $\mathcal{E}$ . If the polynomial  $\Psi$  is nonzero then we have the following bound for the cardinality of the set  $\mathcal{E}$

$$|\mathcal{E}| \leq (D - 1 + (k+1)t(B-1))/D < \frac{(k+1)tB}{[(t|T|/(2kB^{2k}))^{1/2}]}$$

Besides an analog of inequality (39) is

$$2sD^2 \leq 2sD(t|T|/(2kB^{2k}))^{1/2} < DB^{k+1}, \quad (43)$$

where the second inequality from (40) was used. By (40) and  $|T| \leq tk/2$ , we find that

$$t \geq DB^k + \frac{\frac{k}{2}D^2B^{2k}}{|T| - k + 1}.$$

Using condition (41) and applying Proposition 3.7 with  $n = k$ , we obtain that for some different  $\mu_j \in T$ ,  $j \in [k]$ , the polynomial  $\Psi(X)$  is nonzero identically. That concludes the proof.  $\square$

*Note 4.3* Though sum (42) in Statement 4.2 considered for specific tuple of elements  $\mu_j$  the dependence between parameters  $B, t$  and  $T$  (see the first inequality from (40)) not so onerousness as bound (33) of Lemma 4.1.

**Corollary 4.4** Let  $R \subseteq \mathbb{Z}_p^*$  be a multiplicative subgroup,  $k \geq 1$  a positive integer. Let also  $T \subseteq \mathbb{Z}_p^*$  be any set,  $2k \leq |T| \leq |R|k/2$ ,  $Q = RQ$  be a  $R$ -invariant set,  $0 \notin Q$ ,

$$|Q| < \left(\frac{k|R|}{2|T|}\right)^{1/2} \left( \left(\frac{|R||T|}{8k}\right)^{1/2k} - 1 \right)^{2k+1} \quad (44)$$

and

$$p \geq \left(\frac{k|R|^3|T|}{2}\right)^{1/2} \left( \left( |Q| \left(\frac{2|T|}{k|R|}\right)^{1/2} \right)^{1/(2k+1)} + 1 \right). \quad (45)$$

Then

$$\begin{aligned} & \min_{\mu_1, \dots, \mu_k \in T, \mu_i \neq \mu_j} C_{k+1}(Q, R, \dots, R)(\mu_1, \dots, \mu_k) \leq \\ & \leq (32k^3)^{1/2} \left(\frac{|R|}{|T|}\right)^{1/2} \left( \left( |Q| \left(\frac{2|T|}{k|R|}\right)^{1/2} \right)^{1/(2k+1)} + 1 \right)^{k+1}. \end{aligned}$$

**Proof.** Let  $t = |R|$ ,  $s = |Q|/t$ . Let  $B$  be the least integer such such that  $B^{2k+1} > 2s \left(\frac{t|T|}{2k}\right)^{1/2}$ . Then  $B \leq \left(2s \left(\frac{t|T|}{2k}\right)^{1/2}\right)^{1/(2k+1)} + 1$ . Since  $|Q| < \left(\frac{kt}{2|T|}\right)^{1/2} \left( \left(\frac{|R||T|}{8k}\right)^{1/2k} - 1 \right)^{2k+1}$  it follows

that

$$2kB^{2k} \leq 8kB^{2k} \leq 8k \left( \left( 2s \left( \frac{t|T|}{2k} \right)^{1/2} \right)^{1/(2k+1)} + 1 \right)^{2k} < t|T|. \quad (46)$$

Thus all conditions (40) of Statement 4.2 are satisfied. Inequality (41) of the lemma is a consequence of bound (45). Using Statement 4.2 and (46), we obtain

$$\begin{aligned} \min_{\mu_1, \dots, \mu_k \in T} C_{k+1}(Q, R, \dots, R)(\mu_1, \dots, \mu_k) &\leq \frac{(k+1)tB}{[(t|T|/(2kB^{2k}))^{1/2}]} \leq (8k)^{1/2}(k+1) \left( \frac{t}{|T|} \right)^{1/2} B^{k+1} \\ &\leq (32k^3)^{1/2} \left( \frac{t}{|T|} \right)^{1/2} \left( \left( |Q| \left( \frac{2|T|}{k|R|} \right)^{1/2} \right)^{1/(2k+1)} + 1 \right)^{k+1}. \end{aligned}$$

This completes the proof.  $\square$

*Note 4.5* One can generalize Corollary 4.4 consider the sum  $\sum_{\lambda \in Q_1} C_{k+1}(Q, R, \dots, R)(\mu_1, \dots, \mu_k)$ ,  $Q_1 = RQ_1$  as in Theorem 1.1. We do not need in the generalization.

### 5. On subgroups sumsets.

First of all we write simple consequences of Lemma 4.1 and Theorem 1.1.

**Corollary 5.1** *Let  $R \subseteq \mathbb{Z}_p^*$  be a multiplicative subgroup, and  $Q, Q_1, Q_2 \subseteq \mathbb{Z}_p^*$  be arbitrary  $R$ -invariant sets. Then*

1) *If  $|Q| \ll |R|^3$ ,  $|Q||R|^3 \ll p^3$  then*

$$\sum_{x \in Q} (R \circ R)(x) \ll |R||Q|^{2/3}. \quad (47)$$

2) *If  $|Q||Q_1| \ll |R|^4$ ,  $|Q||Q_1||R|^2 \ll p^3$  then*

$$\sum_{x \in Q} (Q_1 \circ R)(x) \ll |R|^{1/3}(|Q||Q_1|)^{2/3}. \quad (48)$$

3) *If  $|Q||Q_1||Q_2| \ll |R|^5$ ,  $|Q||Q_1||Q_2||R| \ll p^3$  then*

$$\sum_{x \in Q} (Q_1 \circ Q_2)(x) \ll |R|^{-1/3}(|Q||Q_1||Q_2|)^{2/3}. \quad (49)$$

*Note 5.2* Clearly, inequality (49) can be improved provided that some information of the set  $\bigcup_{q \in Q} (q^{-1}Q_1 \times q^{-1}Q_2)$  (which is a multiplicative analog of the set from (7)) is known.

Corollary 5.1 implies a statement about additive energy of any  $R$ -invariant set. The statement is a tiny generalization of a result from [13]. Applying Statement 5.3 below it is easy to obtain (using Lemma 2.3, for example) that any  $R$ -invariant set  $Q \subseteq \mathbb{Z}_p^*$ , such that  $|Q| \ll |R|^{3/2}$ ,  $|Q||R|^{1/2} \ll p$  has the extension property, namely,  $|Q \pm Q| \gg |Q||R|^{1/2}$ .

**Statement 5.3** *Let  $R \subseteq \mathbb{Z}_p^*$  be a multiplicative subgroup, and  $Q \subseteq \mathbb{Z}_p^*$  be an arbitrary  $R$ -invariant set. Let also  $|Q| \ll |R|^{3/2}$ , and  $|Q||R|^{1/2} \ll p$ . Then*

$$E(Q) \ll \frac{|Q|^3}{|R|^{1/2}} \quad \text{and} \quad \max_{\xi \neq 0} |\widehat{Q}(\xi)| \ll |Q|^{7/8} |R|^{-1/4} p^{1/8}. \quad (50)$$

**Proof.** Let  $a$  be a parameter. We have

$$E(Q) \leq a|Q|^2 + \sum_{x : (Q \circ Q)(x) \geq a} (Q \circ Q)^2(x).$$

Let us arrange values  $(Q \circ Q)(x)$ ,  $x \in \mathbb{Z}_p/R$  in decreasing order and denote its values as  $N_1 \geq N_2 \geq \dots$ . Using formula (49) of Corollary 5.1, we get  $N_j \ll |Q|^{4/3}|R|^{-2/3}j^{-1/3}$ . Hence

$$E(Q) \ll a|Q|^2 + |R| \sum_{j : j \ll |Q|^4/(|R|^2 a^3)} j^{-2/3} \cdot \frac{|Q|^{8/3}}{|R|^{4/3}} \ll a|Q|^2 + \frac{|Q|^4}{|R|a}.$$

Putting  $a = |Q|/|R|^{1/2}$ , we obtain the required result. The second inequality in (50) is a consequence of the first one, see e.g. the proof of Corollary 2.5 from [14].  $\square$

We need in a lemma from [14].

**Lemma 5.4** *Let  $R \subseteq \mathbb{Z}_p^*$  be a multiplicative subgroup,  $|R| \ll p^{2/3}$ . Then*

$$E_3(R) \ll |R|^3 \log |R|.$$

Let us obtain a new result on doubling constant of multiplicative subgroups.

**Theorem 5.5** *Let  $R \subseteq \mathbb{Z}_p^*$  be a multiplicative subgroup. If  $|R| \ll p^{1/2}$  then*

$$|R \pm R| \gg \frac{|R|^{5/3}}{\log^{1/2} |R|}. \quad (51)$$

**Proof.** Let  $S = (R - R) \setminus \{0\}$  (for  $R + R$  we use similar arguments). Using Lemma 2.3 and Corollary 2.7, we get

$$|R|^6 \leq E_3(R) \cdot \sum_{x \in S} (S \circ S)(x).$$

If  $|S| \gg |R|^{5/3}$  then it is nothing to prove. In the opposite case, we have  $|S|^3 |R| \ll p^3$ , because of the assumption  $|R| \ll p^{1/2}$ . Using bound (49) of Corollary 5.1 with  $Q = Q_1 = Q_2 = S$ , and Lemma 5.4, we get

$$|R|^6 \ll |R|^3 \log |R| \cdot |S|^2 |R|^{-1/3}.$$

Hence  $|S| \gg |R|^{5/3} \log^{-1/2} |R|$ . Theorem is proved.  $\square$

Inequality (51) answered on a question of article [7]. A weaker bound for subgroups such that  $|R| \ll \sqrt{p}$ , better than (3) was obtained by T. Schoen and the second author in [14]. The strongest result on the cardinality of  $R \pm R$ , where  $\sqrt{p} \ll |R| \ll p^{2/3}$ , is contained in [14]. Let us note a consequence of the theorem above.

**Corollary 5.6** *Let  $R \subseteq \mathbb{Z}_p^*$  be a multiplicative subgroup, and  $\kappa > \frac{33}{67}$  be a real number. Suppose that  $|R| \geq p^\kappa$ . Then for all sufficiently large  $p$  the following holds  $\mathbb{Z}_p^* \subseteq 6R$ .*

Corollary 5.6 is a consequence of Theorem 5.5 and can be proved exactly as Theorem 4.1 from [14], where the inclusion  $\mathbb{Z}_p^* \subseteq 6R$  was obtained under the assumption  $\kappa > \frac{41}{83}$ . Note that a result of A.A. Glibichuk [12] (see also [25]) implies that  $|4R| > p/2$  (and hence  $8R = \mathbb{Z}_p$ ), provided by  $|R| > \sqrt{p}$ .



# References

- [1] *Bolibrukh A.A.*, The inverse monodromy problems in analytical theory of differential equations / M.: MCNMO, 2009.
- [2] *J. Bourgain*, Exponential sums estimates over subgroups and almost subgroups of  $\mathbb{Z}_q^*$ , where  $q$  is composite with few prime factors // GAFA, preprint.
- [3] *J. Bourgain*, Multilinear exponential sums in prime fields under optimal entropy condition on the sources // preprint.
- [4] *J. Bourgain, A. Glibichuk, S. Konyagin*, Estimate for the number of sums and products and for exponential sums in fields of prime order // J. London Math. Soc. (2) 73 (2006), 380–398.
- [5] *J. Bourgain, S. Konyagin*, Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order // CR Acad. Sci., Paris 337 (2003), no 2, 75–80.
- [6] *T. Cochrain, C. Pinner*, Stepanov’s method applied to binomial exponential sums // preprint.
- [7] *T. Cochrain, C. Pinner*, Sum–product estimates applied to Waring’s problem mod  $p$  // preprint.
- [8] *A. Garcia, J.F. Voloch*, Fermat curves over finite fields // J. Number Theory **30** (1988), 345–356.
- [9] *D. R. Heath-Brown, S. Konyagin*, New bounds for Gauss sums derived from  $k$ th powers, and for Heilbronn’s exponential sum // Quart. J. Math. 51 (2000), 221–235.
- [10] *S. Konyagin, I. Shparlinski*, Character sums with exponential functions / Cambridge University Press, Cambridge, 1999.
- [11] *A. A. Glibichuk, S. V. Konyagin*, Additive properties of product sets in fields of prime order // arXiv:math.NT/0702729.
- [12] *A. A. Glibichuk*, Combinatorial properties of sets of residues modulo a prime and the Erdős-Graham problem // Mat. Zametki, 79 (2006), 384–395; translation in: Math. Notes 79 (2006), 356–365.
- [13] *S. V. Konyagin*, Estimates for trigonometric sums and for Gaussian sums // IV International conference ”Modern problems of number theory and its applications”. Part 3 (2002), 86–114.
- [14] *T. Schoen, I.D. Shkredov* Additive properties of multiplicative subgroups of  $\mathbb{F}_p$  // Quartarely Journal of Mathematics, accepted for publication, available at arXiv:1008.0723v1 [math.NT] 4 Aug 2010.
- [15] *S.A. Stepanov* On the number of points on hyperelliptic curve over prime finite field // IAN **33** (1969), 1171–1181.

- [16] *I. D. Shkredov*, On some additive problems concerning exponential function // Uspehi Mat. Nauk **58**, 4, 165–166, 2003.
- [17] *T. Tao, V. Vu*, Additive combinatorics / Cambridge University Press 2006.
- [18] *S. Yekhanin*, A Note on Plane Pointless Curves // preprint.
- [19] *W. Rudin*, Fourier analysis on groups / Wiley 1990 (reprint of the 1962 original).
- [20] *N. H. Katz, P. Koester*, On additive doubling and energy // arXiv:0802.4371v1.
- [21] *T. Sanders*, On a non-abelian Balog–Szemerédi–type lemma // arXiv:0912.0306.
- [22] *T. Sanders*, Structure in sets with logarithmic doubling // arXiv:1002.1552.
- [23] *T. Sanders*, On Roth’s theorem on progressions // arXiv:1011.0104v1 [math.CA] 30 Oct 2010.
- [24] *T. Schoen*, Near optimal bounds in Freiman’s theorem // Duke Math. Journal, to appear.
- [25] *M. Rudnev*, An improved estimate on sums of product sets // arXiv:0805.2696.